

Purple Teaming for Blue Teams

SEC501

Stop guessing if your detections actually work. Run realistic purple team exercises to validate, improve, and measure your detection coverage across Microsoft Sentinel, Defender XDR, and open-source SIEMs.

Modules	24
Lessons	247
Phases	3
Free preview	Course Orientation (7 lessons)

The method

The course argument is that a detection nobody has fired is an untested assumption. Every technique across the ATT&CK tactics runs the same five-step cycle in a lab you build.

1. Simulate. Execute the technique yourself so you know exactly what happened and when. Reading about it tells you the outcome, not the footprint.
2. Investigate. Follow it through the telemetry it produced, and find which sources saw it and which were blind. The blind ones are the finding.
3. Detect. Write the rule against the durable artifact the technique leaves, not against the tool that created it this time.
4. Tune. Measure the alert volume, exclude the legitimate activity, and accept that every exclusion is a new blind spot you now own.
5. Validate. Re-run the technique to prove the rule fires. Then ask how you would bypass your own rule, and close that gap before somebody else finds it.

The capstone chains it: a full intrusion emulated end to end, then reported as a coverage figure with a stated denominator and a remediation plan somebody could fund.

What this course assumes

No minimum experience and no prerequisite course, and no offensive background assumed. The lab is built from nothing across four environments and three SIEMs.

What makes it go faster: a machine with enough memory to run several virtual machines, and comfort at a command line. The lab build is taught in full, including the telemetry settings that are off by default and decide every result after them.

What this course does not cover: penetration testing as a profession, exploit development and red team tradecraft. Attack technique here exists to test a detection.

Full syllabus

Phase 1: Foundations and Lab Build

Course Orientation [FREE PREVIEW](#)

What Purple Teaming for Blue Teams teaches: stop assuming your detections fire and prove it.

1. PT0.1 How Real Incidents Actually Unfold, and What Your Rules Miss
2. PT0.2 The Purple-Team Mindset
3. PT0.3 The Vocabulary of Coverage
4. PT0.4 The Toolkit and What Comes Next
5. Module Summary
6. Check My Knowledge
7. Sample Technique Sub. T1059.001 PowerShell (Preview from Module 3)

Building Your Purple-Team Lab

Build a four-environment, three-SIEM purple-team lab from scratch.

1. PT1.1 Why a Local Lab, and Why Not Your Work Environment
2. PT1.2 Hypervisor and VM Setup
3. PT1.3 Windows Endpoint Build with Sysmon
4. PT1.4 Active Directory Domain Controller Build
5. PT1.5 Joining the Endpoint to the Domain
6. PT1.6 Linux VM Build with auditd
7. PT1.7 M365 Developer Tenant Configuration
8. PT1.8 Azure Subscription, Sentinel, and Log Analytics
9. PT1.9 Defender XDR Advanced Hunting
10. PT1.10 Secondary SIEM. Splunk Free
11. PT1.11 Secondary SIEM. Elastic Stack
12. PT1.12 Smoke Test. Fire Your First Technique
13. Module Summary
14. Check My Knowledge

Phase 2: Walking the ATT&CK Kill Chain

Initial Access, How Attackers Get In

Walk six initial access techniques end-to-end: spearphishing links and attachments, stolen cloud credentials, exploited public-facing applications, compromised remote services, and abused trust relationships.

1. PT2.1 Phishing: Spearphishing Link (T1566.002)
2. PT2.2 Phishing: Spearphishing Attachment (T1566.001)
3. PT2.3 Valid Accounts: Cloud Accounts (T1078.004)
4. PT2.4 Exploit Public-Facing Application (T1190)
5. PT2.5 External Remote Services (T1133)
6. PT2.6 Trusted Relationship (T1199)
7. PT2.7 Drive-by Compromise (T1189)
8. PT2.8 Phishing via Service (T1566.003)
9. PT2.9 Module Deliverable. Initial Access Coverage Report
10. Module Summary
11. Check My Knowledge

Execution, How Attackers Run Code

Walk ten execution techniques end-to-end across Windows, Linux, Active Directory, and Microsoft 365.

1. PT3.1 Command and Scripting Interpreter: PowerShell (T1059.001)
2. PT3.2 Command and Scripting Interpreter: Windows Command Shell (T1059.003)
3. PT3.3 Command and Scripting Interpreter: Unix Shell (T1059.004)
4. PT3.4 Command and Scripting Interpreter: Visual Basic (T1059.005)
5. PT3.5 Command and Scripting Interpreter: Python (T1059.006)
6. PT3.6 Command and Scripting Interpreter: JavaScript (T1059.007)
7. PT3.7 Windows Management Instrumentation (T1047)
8. PT3.8 Scheduled Task/Job: Scheduled Task (T1053.005)
9. PT3.9 User Execution: Malicious File (T1204.002)
10. PT3.10 Inter-Process Communication: Component Object Model (T1559.001)
11. PT3.11 Module Deliverable. Execution Coverage Report
12. Module Summary
13. Check My Knowledge

Persistence, How Attackers Stay

Walk twelve persistence techniques end-to-end across Windows, Linux, Active Directory, and Microsoft 365.

1. PT4.1 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
2. PT4.2 Scheduled Task/Job: Scheduled Task. Persistence Focus (T1053.005)
3. PT4.3 Event Triggered Execution: WMI Event Subscription (T1546.003)
4. PT4.4 Account Manipulation: Device Registration (T1098.005)
5. PT4.5 Account Manipulation: SSH Authorized Keys (T1098.004)
6. PT4.6 Create Account: Local Account (T1136.001)
7. PT4.7 Create or Modify System Process: Windows Service (T1543.003)
8. PT4.8 Event Triggered Execution: Change Default File Association (T1546.001)
9. PT4.9 Account Manipulation: Additional Cloud Credentials (T1098.001)
10. PT4.10 Event Triggered Execution: Unix Shell Configuration Modification (T1546.004)
11. PT4.11 Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
12. PT4.12 Office Application Startup: Office Template Macros (T1137.001)
13. PT4.13 Module Deliverable. Persistence Coverage Report
14. Module Summary
15. Check My Knowledge

Privilege Escalation, How Attackers Elevate

Walk twelve privilege escalation techniques end-to-end across Windows, Linux, Active Directory, and Microsoft 365.

1. PT5.1 Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
2. PT5.2 Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003)
3. PT5.3 Access Token Manipulation: Token Impersonation/Theft (T1134.001)
4. PT5.4 Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001)
5. PT5.5 Valid Accounts: Domain Accounts (T1078.002)
6. PT5.6 Process Injection: DLL Injection (T1055.001)
7. PT5.7 Account Manipulation: Additional Cloud Roles (T1098.003)
8. PT5.8 Access Token Manipulation: Parent PID Spoofing (T1134.004)
9. PT5.9 Process Injection: Thread Execution Hijacking (T1055.003)
10. PT5.10 Hijack Execution Flow: DLL Side-Loading (T1574.002)
11. PT5.11 Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)
12. PT5.12 Access Token Manipulation: SID-History Injection (T1134.005)
13. PT5.13 Module Deliverable. Privilege Escalation Coverage Report
14. Module Summary
15. Check My Knowledge

Defense Evasion, How Attackers Break Your Detections

Walk ten defense evasion techniques that exist to defeat the detection rules you built in Modules 2–5.

1. PT6.1 Impair Defenses: Disable or Modify Tools (T1562.001)
2. PT6.2 Indicator Removal: Clear Windows Event Logs (T1070.001)
3. PT6.3 Obfuscated Files or Information: Command Obfuscation (T1027.010)
4. PT6.4 System Binary Proxy Execution: Rundll32 (T1218.011)
5. PT6.5 Impair Defenses: Disable Windows Event Logging (T1562.002)
6. PT6.6 Masquerading: Match Legitimate Name or Location (T1036.005)
7. PT6.7 Hide Artifacts: Hidden Files and Directories (T1564.001)
8. PT6.8 Indicator Removal: File Deletion (T1070.004)
9. PT6.9 Impair Defenses: Disable or Modify System Firewall (T1562.004)
10. PT6.10 Use Alternate Authentication Material: Pass the Hash (T1550.002)
11. PT6.11 Module Deliverable. Defense Evasion Coverage Report
12. Module Summary
13. Check My Knowledge

Credential Access, How Attackers Harvest Authentication Material

Walk twelve credential access techniques that harvest passwords, hashes, tokens, and session cookies from Windows, Active Directory, Microsoft 365, and Linux.

1. PT7.1 OS Credential Dumping: LSASS Memory (T1003.001)
2. PT7.2 OS Credential Dumping: NTDS.dit (T1003.003)
3. PT7.3 OS Credential Dumping: DCSync (T1003.006)
4. PT7.4 Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
5. PT7.5 Steal Web Session Cookie (T1539)
6. PT7.6 Credentials from Password Stores: Web Browsers (T1555.003)
7. PT7.7 Unsecured Credentials: Credentials in Files (T1552.001)
8. PT7.8 Brute Force: Password Spraying (T1110.003)
9. PT7.9 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning (T1557.001)
10. PT7.10 OS Credential Dumping: /etc/shadow (T1003.008)
11. PT7.11 Steal Application Access Token (T1528)
12. PT7.12 Modify Authentication Process: Multi-Factor Authentication (T1556.006)
13. PT7.13 Module Deliverable. Credential Access Coverage Report
14. Module Summary
15. Check My Knowledge

Discovery, How Attackers Map the Environment Before Moving

Walk five discovery techniques that enumerate accounts, systems, groups, cloud services, and files across Windows, Active Directory, Microsoft 365, and Linux.

1. PT8.1 Account Discovery: Local and Domain Accounts (T1087.001/.002)
2. PT8.2 Remote System Discovery (T1018)
3. PT8.3 Permission Groups Discovery: Local and Domain Groups (T1069.001/.002)
4. PT8.4 Cloud Service Discovery (T1526)
5. PT8.5 File and Directory Discovery (T1083)
6. PT8.6 Domain Trust Discovery (T1482)
7. PT8.7 System Network Configuration Discovery (T1016)
8. PT8.8 System Network Connections Discovery (T1049)
9. PT8.9 System Owner/User Discovery (T1033)
10. PT8.10 System Information Discovery (T1082)
11. PT8.11 Network Share Discovery (T1135)
12. PT8.12 Cloud Infrastructure Discovery (T1580)
13. PT8.13 Module Deliverable. Discovery Coverage Report
14. Module Summary
15. Check My Knowledge

Lateral Movement, How Attackers Convert Access into Reach

Walk twelve lateral movement techniques that move attackers across Windows, Active Directory, Microsoft 365, and Linux using legitimate protocols.

1. PT9.1 Remote Services: Remote Desktop Protocol (T1021.001)
2. PT9.2 Remote Services: SMB/Windows Admin Shares (T1021.002)
3. PT9.3 Remote Services: Windows Remote Management (T1021.006)
4. PT9.4 Remote Services: Distributed Component Object Model (T1021.003)
5. PT9.5 Remote Services: SSH (T1021.004)
6. PT9.6 Use Alternate Authentication Material: Pass the Hash (T1550.002)
7. PT9.7 Use Alternate Authentication Material: Pass the Ticket (T1550.003)
8. PT9.8 Internal Spearphishing (T1534)
9. PT9.9 Remote Service Session Hijacking: RDP Hijacking (T1563.002)
10. PT9.10 Lateral Tool Transfer (T1570)
11. PT9.11 Software Deployment Tools (T1072)
12. PT9.12 Taint Shared Content (T1080)
13. PT9.13 Module Deliverable. Lateral Movement Coverage Report
14. Module Summary
15. Check My Knowledge

Collection, How Attackers Harvest What They Came For

Walk twelve collection techniques that gather email, files, credentials, screen content, and cloud data across Windows, Microsoft 365, and Linux.

1. PT10.1 Archive Collected Data: Archive via Utility (T1560.001)
2. PT10.2 Email Collection: Local Email Collection (T1114.001)
3. PT10.3 Email Collection: Remote Email Collection (T1114.002)
4. PT10.4 Automated Collection (T1119)
5. PT10.5 Data from Information Repositories: SharePoint (T1213.003)
6. PT10.6 Data from Local System (T1005)
7. PT10.7 Data Staged: Local Data Staging (T1074.001)
8. PT10.8 Screen Capture (T1113)
9. PT10.9 Video Capture (T1125)
10. PT10.10 Input Capture: Keylogging (T1056.001)
11. PT10.11 Data from Cloud Storage Object (T1530)
12. PT10.12 Data from Network Shared Drive (T1039)
13. PT10.13 Module Deliverable. Collection Detection Program Template
14. Module Summary
15. Check My Knowledge

Command and Control, How Attackers Maintain Their Lifeline

Detect and analyze twelve C2 communication techniques across HTTP/S, DNS, tunneling, proxy, encoding, and protocol impersonation channels.

1. PT11.1 Application Layer Protocol: Web Protocols (T1071.001)
2. PT11.2 Application Layer Protocol: DNS (T1071.004)
3. PT11.3 Protocol Tunneling (T1572)
4. PT11.4 Encrypted Channel: Asymmetric Cryptography (T1573.002)
5. PT11.5 Application Layer Protocol: Mail Protocols (T1071.003)
6. PT11.6 Web Service (T1102)
7. PT11.7 Dynamic Resolution: Domain Generation Algorithms (T1568.002)
8. PT11.8 Proxy: Internal Proxy (T1090.001)
9. PT11.9 Proxy: External Proxy (T1090.002)
10. PT11.10 Non-Application Layer Protocol (T1095)
11. PT11.11 Data Encoding: Standard Encoding (T1132.001)
12. PT11.12 Data Obfuscation: Protocol Impersonation (T1001.003)
13. PT11.13 Module Deliverable. C2 Detection Matrix
14. Module Summary
15. Check My Knowledge

Exfiltration, How Attackers Get the Data Out

Validate detection coverage across twelve exfiltration techniques, from C2-channel piggyback and cloud storage abuse to DNS tunneling, webhook endpoints, USB media, and automated pipelines.

1. PT12.1 Exfiltration Over C2 Channel (T1041)
2. PT12.2 Exfiltration to Cloud Storage (T1567.002)
3. PT12.3 Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)
4. PT12.4 Exfiltration Over Encrypted Non-C2 Protocol (T1048.001)
5. PT12.5 Exfiltration to Code Repository (T1567.001)
6. PT12.6 Transfer Data to Cloud Account (T1537)
7. PT12.7 DNS Exfiltration (T1048.002)
8. PT12.8 Data Transfer Size Limits (T1030)
9. PT12.9 Scheduled Transfer (T1029)
10. PT12.10 Exfiltration Over Webhook (T1567.004)
11. PT12.11 Automated Exfiltration (T1020)
12. PT12.12 Exfiltration Over Physical Medium: USB (T1052.001)
13. PT12.13 Module Deliverable. Exfiltration Detection Coverage Map
14. Module Summary
15. Check My Knowledge

Impact, How Attackers Deliver the Final Blow

Detect and contain twelve impact techniques, from ransomware encryption and wiper attacks to recovery inhibition, account lockout, data manipulation, and resource hijacking.

1. PT13.1 Data Encrypted for Impact (T1486)
2. PT13.2 Inhibit System Recovery (T1490)
3. PT13.3 Service Stop (T1489)
4. PT13.4 Account Access Removal (T1531)
5. PT13.5 Data Destruction (T1485)
6. PT13.6 External Defacement (T1491.002)
7. PT13.7 Disk Wipe: Disk Structure Wipe (T1561.002)
8. PT13.8 System Shutdown/Reboot (T1529)
9. PT13.9 Resource Hijacking (T1496)
10. PT13.10 Data Manipulation: Stored Data (T1565.001)
11. PT13.11 Network Denial of Service: Direct Network Flood (T1498.001)
12. PT13.12 Firmware Corruption (T1495)
13. PT13.13 Module Deliverable. Impact Detection and Containment Matrix
14. Module Summary
15. Check My Knowledge

Phase 3: Capstone

Capstone, CHAIN-HARVEST Full-Chain Purple-Team Exercise

Execute the complete CHAIN-HARVEST AiTM attack chain across all four environments and three SIEMs.

1. PT14.1 CHAIN-HARVEST Scenario Briefing (INC-2026-0227)
2. PT14.2 Phase 1: Initial Access and Execution (T1566.002 → T1059.001)
3. PT14.3 Phase 2: Persistence and Privilege Escalation (T1098.005 → T1548.002)
4. PT14.4 Phase 3: Defense Evasion and Credential Access (T1562.001 → T1003.001)
5. PT14.5 Phase 4: Discovery and Lateral Movement (T1087.002 → T1021.002)
6. PT14.6 Phase 5: Collection and Exfiltration (T1560.001 → T1567.002)
7. PT14.7 Phase 6: Impact. Recovery Inhibition and Ransomware (T1490 → T1486)
8. PT14.8 Detection Coverage Assessment
9. PT14.9 Gap Analysis and Remediation Planning
10. PT14.10 Building the Purple-Team Program
11. PT14.11 Writing the Purple-Team Report
12. PT14.12 Full-Chain Exercise. CHAIN-HARVEST End-to-End
13. PT14.13 Module Deliverable. CHAIN-HARVEST Purple-Team Report
14. Module Summary
15. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The lookup layer: every emulation command and validation query the course teaches, grouped by the question you are asking at the moment you open the page.

1. Telemetry Preflight
2. Initial Access and Execution
3. Persistence and Privilege Escalation
4. Defense Evasion and Credential Access
5. Discovery and Lateral Movement
6. Collection, Command and Control, and Exfiltration
7. Impact
8. Did the Detection Fire
9. Why the Rule Stayed Silent
10. Coverage Arithmetic
11. Cleanup

Cookbooks

Procedures: what you do, in what order, what each step must produce, and where it branches.

1. Planning and Authorizing an Exercise
2. Preparing the Environment and Verifying Telemetry
3. Executing a Technique and Recording the Result
4. Validating the Detection
5. Diagnosing a Rule That Stayed Silent
6. Writing or Tuning the Rule, Then Re-testing
7. Measuring Coverage and Reporting

Lab Setup

The build-and-verify reference for the emulation lab: what the environment has to produce, the settings that are off by default and decide every later result, the activity generation that gives you something to detect, and the verification that fails loudly.

1. The Hosts You Need
2. Turning On What Is Off
3. The Toolchain and Documented Swaps
4. Generating a Baseline
5. Verification and Retention Limits

Walkthroughs

Exercises worked end to end, including the wrong turns: the technique run, the rule that did or did not fire, the diagnosis, the rule change, and the re-test that settled it.

1. The Rule That Was Never On
2. The Detection That Fired for the Wrong Reason
3. The Detection That Caught the Wrong Thing
4. The Gap That Was a Collection Problem
5. The Alert Nobody Worked
6. The Compound Rule That Earned Its Place
7. The Quarter That Rediscovered Its Own Findings

Playbooks

Emulation procedures opened at the moment you are about to run a technique family: prerequisites, pre-flight, time budget, the execution sequence, the validation, and the tiered disposition of the result.

1. Credential Access
2. Persistence
3. Initial Access
4. Execution and Defense Evasion
5. Discovery and Lateral Movement
6. Collection, Exfiltration and Impact
7. Command and Control

Playground

Where to practice purple teaming beyond the course: the detection library, the Splunk Lab, the SOC Simulator and the open-source emulation frameworks, with an honest note on which of them is written for this course and which is not.

Operational Reference

The emulation commands, detection rules and telemetry indicators from every module in one place, indexed by ATT&CK tactic.

1. Purple Team Quick Reference

References & Further Reading

Where to check whether anything in this course has changed: the ATT&CK releases the technique set tracks, the emulation framework documentation, the Sigma rule sources, and the detection community work cited throughout the course.

Course Completion

Course Exam

You've reached the end of Purple Teaming for Blue Teams.

1. Course Completion. Purple Teaming for Blue Teams

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/purple-teaming-for-blue-teams/